CLAIM LISTING

This listing of claims will replace all prior versions and listings of claims in the application:

AMENDMENTS TO THE CLAIMS

1. (Original) A programmable logic device (PLD) comprising:

configurable logic configured by a configuration memory;

structure for receiving a bitstream from a source external to the PLD, wherein the bitstream includes unencrypted configuration bits and encrypted configuration bits;

a key memory for storing a decryption key;

a decryptor having a decryption algorithm for decrypting the encrypted configuration bits in the bitstream using the key, and thereby forming configuration data; and

structure for loading the configuration data into the configuration memory.

2. (Original) The PLD of Claim 1 wherein the unencrypted configuration bits are control bits and the encrypted configuration bits are configuration data bits.

3. (Original) A programmable logic device (PLD) comprising:

configurable logic configured by a configuration memory;

structure for receiving a bitstream from a source external to the PLD;

a key memory for storing a decryption key;

a decryptor having a decryption algorithm for decrypting data in the bitstream using the key;

structure for loading the decrypted data into the configuration memory;

structure for reading header information from the bitstream indicating whether the bitstream includes encrypted data; and

structure for directing the bitstream to the decryptor if the header information indicates the bitstream includes encrypted data and bypassing the decryptor if the header information indicates the bitstream does not include encrypted data.

4. (Original) The PLD of Claim 3 further comprising:

structure for reading back configuration from the configuration memory; and

structure for disabling the structure for reading back configuration when the header information indicates the bitstream includes encrypted data.

5. (Original) The PLD of Claim 3 further comprising:

structure for reconfiguring the PLD after the PLD has been configured; and

structure for disabling the structure for reconfiguring the PLD when the header information indicates the bitstream includes encrypted data.

6. (Original) A programmable logic device (PLD) comprising:

configurable logic configured by a configuration memory;

structure for receiving a bitstream from a source external to the PLD;

a key memory for storing a plurality of decryption keys, wherein the key memory includes a plurality of registers for storing the plurality of decryption keys;

a decryptor having a decryption algorithm for decrypting data in the bitstream using at least one of the keys; and

structure for loading the decrypted data into the configuration memory.

7. (Original) The PLD of Claim 6 wherein the decryptor reads from one of the registers for storing a plurality of decryption keys a value indicating whether another key will also be used for decryption.

8. (Original) The PLD of Claim 6 wherein the decryptor includes a circuit for aborting decryption if an attempt is made to use the keys differently from the way specified by the keys.

9. (Original) The PLD of Claim 6 wherein a key specifies whether it is a first, middle, last, or only key of a key set.

10. (Original) The PLD of Claim 6 wherein a key specifies whether it is a last key or not a last key of a key set.

11. (Original) The PLD of Claim 6 wherein the PLD reads an address of a key from the bitstream.

12. (Original) The PLD of Claim 6 wherein a first group of words in the bitstream is encrypted with a first key known to a first designer and a second group of words in the bitstream is encrypted with a second key known to a second designer.

13. (Original) The PLD of Claim 1 further comprising structure for placing the key memory into a secure mode and a non-secure mode, and wherein keys are loaded while the key memory is in the non-secure mode.

14. (Original) The PLD of Claim 13 wherein the keys can be read while the key memory is in the non-secure mode.

15. (Original) The PLD of Claim 14 wherein moving the key memory from the secure mode to the non-secure mode causes all keys to be erased.

16. (Original) The PLD of Claim 15 wherein moving the key memory from the secure mode to the non-secure mode also causes the configuration data to be erased.

17. (Original) The PLD of Claim 1 wherein the bitstream comprises a plurality of words of data, and the decryption algorithm uses both the key and a previously decrypted word of the configuration data for decrypting a current word of the encrypted configuration bits.

18-25. (Cancelled)

26. (Original) A programmable logic device (PLD) comprising:

configurable logic configured by a configuration memory;

structure for receiving a bitstream from a source external to the PLD;

a key memory for storing a decryption key;

a decryptor having a decryption algorithm for decrypting encrypted configuration bits in the bitstream using the key, and thereby forming configuration data; and

structure for loading the configuration data into the configuration memory.

27. (Original) The PLD of claim 26 wherein the structure for loading the configuration data into the configuration memory includes a CRC checksum calculation circuit.

28. (New) A programmable logic device (PLD), comprising:

a configuration memory;

programmable logic circuitry coupled to the configuration memory;

a decryptor circuit coupled to the configuration control circuit and adapted to decrypt input data and output decrypted data; and

a configuration control circuit coupled to the configuration memory, to the decryptor circuit, and to a configuration input port, the configuration control circuit adapted to receive configuration data via the input port, transmit an first portion of the configuration data to the decryptor circuit responsive to a code in a second portion of the configuration data having a first value, and load the configuration memory with decrypted data from the decryptor circuit.

29. (New) The PLD of claim 28, further comprising a key storage element coupled to the decryptor circuit and adapted for storage of at least one decryption key.

30. (New) The PLD of claim 28, wherein the configuration control circuit is further adapted to bypass transmission of the first portion of the configuration data to the decryptor circuit responsive to the code having a second value.

31. (New) The PLD of claim 28, wherein the configuration control circuit is further adapted to disable partial reconfiguration of the PLD and disable readback of configuration data from the PLD responsive to input of encrypted configuration data, decryption of the encrypted configuration data, and loading of the configuration memory.

32. (New) The PLD of claim 28, further comprising a key storage element coupled to the decryptor circuit and adapted to store plurality of decryption keys.

33. (New) The PLD of claim 32, wherein the decryptor circuit is adapted to decrypt a single input set of encrypted data using the plurality of encryption keys.

34. (New) The PLD of claim 32, further comprising a key control register coupled to the decryptor circuit, wherein the decryptor circuit is adapted decrypt a single input set of encrypted data using a number of encryption keys from the key memory responsive to a value in the key control register.

35. (New) The PLD of claim 32, wherein the decryptor circuit is adapted to decrypt input encrypted data using one of the plurality of decryption keys addressed by a value in the second portion of the configuration data.